重构图视角下超级账本在物联网的应用研究综述 *

冷泽琪，王坤昊[†]，梁　纬，郑月锋
(吉林师范大学 计算机学院，吉林 四平 136000)

摘　要：在部署基于区块链的物联网应用中，出现了缺少细粒度隐私保护、事务处理效率低、高延迟、灵活性和动态性不足等方面的技术阻碍。为进一步推进区块链技术在物联网的普及和应用落地，致力于企业级标准的区块链技术的超级账本引起了研究界的广泛关注。然而在当前的研究中，缺少针对基于超级账本的物联网的客观综述。本研究旨在以独特的视角回顾超级账本在物联网领域的研究。为展示更直观的差异、提供技术融合流程，本研究提出了重构图的分析方法。重构是将文献中核心设计和原架构图融合，重新构造可以展示文献核心思想图的过程。这种方法旨在将文献的核心思想可视化。最后，从低功耗共识算法、智能交易验证、链上链下混合存储和自定义激励机制四个方向对超级账本在物联网的未来研究进行展望和总结。

关键词：超级账本；物联网；区块链
中图分类号：TP391　　doi: 10.19734/j.issn.1001-3695.2022.01.0040

Survey on application of hyperledger in IoT from perspective of reconstructing diagrams

Leng Zeqi, Wang Kunhao[†], Liang Wei, Zheng Yuefeng
(*College of Computer science*, *Jilin Normal University*, *Siping* 136000, *China*)

Abstract: In the deployment of blockchain-based IoT applications, technical hindrances in terms of lack of fine-grained privacy protection, low transaction processing efficiency, high latency, and lack of flexibility and dynamism have emerged. To further promote the popularization and application of blockchain technology in IoT, the Hyperledger dedicated to the enterprise standard blockchain technology has attracted wide attention from the research community. However, there is a lack of objective review for Hyperledger-based IoT in the current research. This study aimed to review the research on Hyperledger in the IoT domain with a unique perspective. In order to demonstrate more intuitive differences and provide a faster process of technology convergence, this study proposed a reconstruction diagrams analysis method. Reconstruction is the process of merging the core design of a literature with the original architecture and reconstructing the diagram that shows the core idea of the document. This approach aims to visualize the core ideas of the literature. Finally, this article prospects and summarizes the future research of Hyperledger in IoT in four directions: low-power consensus algorithm, intelligent transaction verification, on-chain and off-chain hybrid storage, and custom incentive mechanism.

Key words: hyperledger; IoT; blockchain

0　引言

随着智能设备和高速网络的快速发展，物联网作为资源受限的低功耗网络，其主要标准得到了广泛的接受和普及[1]。然而一些技术的漏洞和缺陷阻碍了物联网的发展，这些阻碍主要集中在集中式服务器带来的数据安全问题和网络拥塞。区块链突破了传统意义的信任，使得网络中的每一项决策从少数节点转变为所有节点共同决定，增加了交易的透明度和存储信任。因此，基于区块链的物联网研究被广泛地探索。这些研究一定程度上解决了物联网数据的安全存储、数据完整性验证等问题。但是区块链技术在隐私保护、负载均衡、网络延迟的缺陷，导致了技术状态无法达到商业应用的标准，尤其是物联网项目。

近年来，超级账本的出现为解决上述问题提供了可能。除了具备区块链一般的特性外，超级账本在四个方面实现了全新的赋能：安全、互操作、共识以及性能。在安全方面：超级账本设计了细粒度的访问控制和私密数据管理，给企业之间提供了隐私保护机制和账本隔离，为企业级的方案提供基础设施。为保障消费者的利益，超级账本支持访问控制的自治性，这使得一些以消费者为中心的应用能够设计与实施。高度模块化的结构使得基于超级账本开发的系统在某个模块或组件发生单点故障时，不会影响系统整体运作。这一特点同时也使超级账本能够更快地与各类系统集成。这些可插拔的组件使得超级账本能够在同一个分布式网络中满足丰富的业务逻辑。在互操作方面：超级账本开发了点对点的身份认证系统，为消费者或企业通过便携式的电子身份执行跨链、跨层或跨系统的操作提供了基础设施。在共识方面：可插拔的共识机制使得不同业务能够在同一个分布式网络中达成共识。目前超级账本所支持的共识算法覆盖了节能、声誉、工作量证明、时间证明、权威、容错、授权权益等方面。因此，显著地提升了超级账本的适用性。在性能方面：网络中的决策由一定数量的节点决定代替了由所有节点共同决定，这将大大减少算力成本并确保信任。超级账本网络可以是动态的，为大量便携式设备的连接提供了可能。超级账本将处理交易的节点细分为四种角色，每种角色都具备不同的功能，并允许开发者根据网络负载调整节点的部署。此外，解耦的排序处理能够解决一定程度的网络拥塞和延迟。

基于超级账本的物联网研究逐年增长，然而目前没有关

收稿日期：2022-01-24；**修回日期：**2022-03-25　**基金项目：**吉林省自然科学基金资助项目(20210101176JC)
作者简介：冷泽琪(1996-)，女，吉林延边朝鲜族自治州人，硕士研究生，主要研究方向为区块链技术；王坤昊(1981-)，男(通信作者)，吉林长春人，副教授，博士，主要研究方向为区块链技术与应用，生物信息学(wkhyoyo@jlnu.edu.cn)；梁纬(1996-)，女，广东广州人，硕士研究生，主要研究方向为图像识别；郑月锋(1978-)，男，吉林吉林人，副教授，博士，主要研究方向为人工智能，大数据技术．

于超级账本在物联网领域的综述。此外，在区块链综述中大部分以文字为主，图表为辅。精炼的语言为研究人员展示了最新的应用进展和趋势，但无法直观地给研究人员展示这些研究的设计思路，研究人员很难从凝练的语言中获取足够的技术融合指南和核心思想。

为更好的解决上述问题，本研究提出一种新的分析方法，即重构图方法。重构图分析方法的主要优势在于二点：一是以最直观的方式展示研究进展和核心思路，突出不同研究之间差异；二是增添了更多的设计细节，将文献中的核心设计可视化。本研究的主要贡献如下：

a) 提出了重构图的分析方法。这项研究考虑了两种情况：第一种是针对没有架构图的文献，提炼文献中的核心设计构造重构图，最大程度地还原作者的核心设计思路。第二种是文献中已有架构图。在文献核心设计的基础上将原架构图重构，增加更多的设计细节。

b) 展示了超级账本在物联网中最新的应用进展。由于现阶段超级账本在物联网的研究比较分散，本研究以应用领域为单位归纳 52 文献。这些应用领域涉及了物联网数据安全、智慧农业和渔业、智能城市监控、智能玩具和 IoT 游戏、智能健身、智慧交通、智慧电网、智慧建筑项目和智慧能源(节能方向)。

1　超级账本技术概述

超级账本致力于开发企业级标准区块链。在官方的概念层面，超级账本是一个“温室”体系，所有的技术由社区开发。并为各个领域的用户、开发商和供应商提供了一个开源且安全的协作环境。因此，超级账本鼓励相似领域中参与者之间的互操作，每个参与者通过沟通获取必要的信息。这种有效的协作方式大大减少了每个参与者的重复工作，使得参与者更有精力去孵化新的想法。为了提高代码质量，超级账本的技术指导委员会(Technical Steering Committee，TSC)定期检查社区的代码和项目，不合格的代码和项目将被抛弃。另外，超级账本鼓励实现专业化[2]，即让更多的人集中精力完成更少的任务，提高参与者的专业程度。发展参与者的专业化还有助于促进知识产权的统一，任何在超级账本社区做贡献的参与者不必担心隐藏的法律问题。

超级账本的通用架构具备 9 个组件：共识层、合约层、通信层、数据存储模块、加密模块、身份服务模块、策略服务模块、应用程序接口(Application Programming Interfaces，APIs)和互操作模块[3]。这些组件构成了高度模块化的结构，任何一个组件的故障不会影响整体的运作。

1.1　赋能技术概述

作为最大的开源项目之一，超级账本目前拥有 18 个顶级项目(包括一项被淘汰的项目)。这些顶级项目为超级账本提供关键技术，也使得超级账本能广泛应用到各个领域中。在技术方面，超级账本涉及了跨系统身份认证、权限控制、多通道(多链)的平台、可视化界面、移动应用、基准测试、密码学库、以太坊客户端及其业务逻辑开发等领域。在应用方面，超级账本已经应用于物联网、数字医疗、供应链追溯、金融、数字证据，人工智能等主流领域。

超级账本将目前的顶级项目分为 4 类，包括 distributed ledgers、domain-specific、libraries 和 tools。每个贡献到超级账本的项目都需要开发者定期维护，这意味着除了维护项目的正常运营，开发者还要及时地为想参与到这个项目的成员解决问题。TSC 会定期审查各个项目的维护情况，并决定项目是否进入下一阶段。当一个项目处于不再推荐使用阶段时，6 个月后该项目会被社区弃用。但弃用的项目信息和部分代码仍然保留在社区中。超级账本中的每个项目必须具备 Modular、Highly secure、Interoperable、Cryptocurrency-agnostic 和 Complete with APIs 五种特征。模块化的组件适用于开发不同需求的分布式解决方案，高度的安全性确保了企业级区块链的实施。互操作性和丰富的 APIs 给大型企业分布式网络提供了轻松的信息交互。

一般情况下，超级账本中的所有项目都要经过 Proposal、incubation、graduated(active)、dormant、deprecated 和 end of life 六个阶段(状态)。各个项目的状态是动态的，并由项目的维护者和 TSC 多次审查共同决定。现阶段，超级账本中的顶级项目只有 2 种状态，分别是 Graduted 和 Incubation。处于 Graduted 状态的项目是目前最活跃、成员数量最多、贡献代码最多的项目。由于不断地更新，活跃项目为超级账本提供了比较成熟的技术和基础设施。根据官网(https://www.hyperledger.org/)所提供的信息，本文剖析了目前处于 Graduted 状态的项目的核心架构及创新设计。

1.1.1 Hyperledger Fabric 概述

Fabric 是超级账本的基石，它的创新设计使得超级账本能够广泛地应用在各个领域中。Fabric 率先引入了权限机制，给各行业的保密交易和账本隔离提供了可能。Fabric 的架构由 Membership services、Certificate authorities(CA)、Nodes、Peers 4 种类型的组件构成。Membership services 主要为区块链节点提供数字证书。CA 为网络中所有节点提供身份证书，这些节点通过私钥和公钥完成交易。Nodes 由被允许加入网络的节点组成，而 Peers 是区块链网络中担任不同任务的角色。

1.1.2 Hyperledger Sawtooth 概述

Sawtooth 的创新设计在于强大的动态性和健壮性。每个 Sawtooth 节点由一个固定部件 validator，和可能的部件 Transaction Processor、REST API、和 Client。在 Sawtooth 网络中，初始节点发送广播包获取附近的节点，邻居节点可以根据规则加入网络，并广播距离自己 1 跳的邻居节点。只要有响应，该节点就可以加入网络。

Sawtooth 架构有 5 个核心组件，包括 peer-to-peer network、distributed log、state machine / smart contract logic layer、distributed state storage、consensus algorithm。peer-to-peer network 允许节点通过 TCP 通信，包括区块、对等体等信息。并且 Sawtooth 网络通过 Gossip protocol 广播事务。Distributed log 包括事务的有序列表，节点根据共识算法将事务排序。Sawtooth 扩展了智能合约的功能，把智能合约视为状态机或事务处理器。Smart contract logic layer 包括一些核心的智能合约(如 Settings、identity、validator registry)和事务家族(如 IntegerKey、BlockInfo、HyperDirectory、Marketplace 等)。Sawtooth 使用 Radix Merkle Tree 的存储结构，它融合了 Radix Tree 和 Merkle Hash Tree 的功能，并且通过这种存储结构存储序列化的合约状态。Consensus 组件提供了共识接口，允许各种共识算法。

1.1.3 Hyperledger Iroha 概述

Iroha 也提供了一种分布式框架，它的特色设计在于权限管理、容错率和性能效率。相对于其他平台，除了节点加入网络需要授权以外，Iroha 的数据读写也要授权。Iroha 允许丰富的内置命令能够更简单地完成资产管理，不同于其他平台中需要预设资产。它设计的容错共识算法 Crash 使得 Iroha 具有更低的延迟。

Iroha 架构有 11 种组件，包括 Torii、MST Processor、Peer Communication Service(PCS)、Ordering Gate、Ordering service、Verified Proposal Creator(VPC)、block creator、Block Consensus (YAC)、Synchronizer、Ametsuchi Blockstore、World State View(WSV)。Torii 负责接收交易并进行预处理，MST Processor 负责转发交易和接收对等体的签名信息。PCS 主要

负责传递交易给 Ordering Gate。Ordering Gate 将与其他对等方验证无状态的交易，对等方中的 Ordering service 创建交易提案(每个节点都包含一个 Ordering service)，并验证该无状态交易是否通过第一次验证。Ordering Gate 收到建议后，将交易转播至 simulator 中的 VPC。VPC 对交易执行状态验证，block creator 将创建新的区块并发送至 YAC 中执行共识。YAC 将最终的消息转发给多个对等方。Synchronizer 负责从 block store 中下载区块，将对等方缺失的区块添加到对等方中。WSV 将展示最新的区块信息。

1.1.4 Hyperledger Indy 概述

Indy 的创新设计在于去中心化的身份认证系统。这种身份认证的核心特征是自我主权身份。这意味着身份一旦被确定，未经身份所有者的允许任何机构和人不得撤销、选择和关联。因此，Indy 可以为用户提供便携式身份证明，并且无须通过第三方集中认证。Indy 网络中只有两种节点，包括验证节点(数量较少)和观察者节点(数量很多)。其中，验证节点负责处理写入请求并参与共识。观察者节点负责读取请求且依赖于信誉等级有机会成为验证节点。

1.1.5 Hyperledger Aries 概述

作为 5 个活跃项目中唯一不是分布式账本平台的技术，Aries 是给去中心化的身份管理和可验证凭证提供安全通信的方法。Aries 有 4 个核心组件，包括 agents、DID communications、protocols 和 key management。Agents 提供了自我主权身份认证的可信代理。用户根据对代理的需求下载或编写相应的代理。比如物联网代理、云代理、协议、规模和隐私性等要求。DID communications 是为多个可信代理提供信息交换，这种信息交换是基于去中心化的协议，它的主要范式是基于消息的(通知)、异步的(请求-响应消息)和单工的。Key management 提供了分布式密钥管理系统，使用三种类型的密钥，包括主密钥、密钥加密密钥和数据密钥。分布式密钥管理系统使得任何身份所有者免遭受第三方机构的中心故障，无须依赖任何组织就能执行网络连接、密钥交换和恢复。

Aries 的出现有助于去中心化的身份认证的实施，点对点的证书认证将根除监控经济。这种认证方法具有高移植性和适用性，用户可以在钱包中存储自己的工作证明或其他身份，并决定哪部分的信息可以被公开查询。

1.1.6 Hyperledger Besu 概述

Besu 是企业级的以太坊平台。Besu 有 7 个核心模块，包括 Ethereum Virtual Machine (EVM)、P2P network、Storage、Permissioning、Privacy、User-facing API 和 Monitoring。在 Privacy 方面，Besu 通过 Tessera 节点确保隐私交互。为了更好地面向企业，Permissioning 启用节点权限和账户权限，只有特定的节点和账户才能访问网络。Storage 存储区块链和世界状态，其中世界状态包括账户状态、账户存储和代码存储。Besu 为用户提供了监控界面，去监控节点和网络。

Besu 支持两种节点类型，包括 Full nodes 和 Archive nodes。Full nodes 只存储当前的区块状态，确保当前的最新状态。Archive nodes 除了存储最新状态，还负责存储自创世区块的所有历史状态。另外，Besu 为用户提供了 3 种 API，包括基于 HTTP/WebSockets 的 JSON-RPC、基于 WebRocket 的 RPC 发布/订阅和基于 HTTP 的 GraphQL。

Besu 能够兼容以太坊主网，支持公有网络和私有网络。给搭建企业级以太坊平台提供了可能。

2　物联网简介

物联网由难度参差不齐的两个部分组成。其中一个细分是人类物联网(IoT)，它是一项重大改进，交互的主导类型是客户端-服务器[4]。IoT 提供日益智能的服务，以满足丰富的语义请求。另一个细分是工业物联网(IIoT)，它旨在用于复杂的任务协同、基于收集数据的决策以及对机械的远程访问[5]。

2.1　IoT 概念简介

物联网是一种新的技术范式，是一个由机器和设备组成的全球网络，能够相互作用和互动。在应用层面，物联网可以根据消费者预先设定的要求完成各种轻型任务。例如，自动扫地、智能化识别、红绿灯的联动等操作。物联网对企业的价值在于连接的设备能够相互通信并与供应商管理的库存系统、客户支持系统、商业智能应用和商业分析整合[6]。

2.2　IIoT 概念简介

工业物联网是将工业知识和经验进行软件化、模型化，是提高制造的效率和质量的技术。在应用层面，工业物联网与物联网最大的不同是它是为重型任务设计的。比如，智能制造、环境监控、智能交通、敌情侦察等。

2.3　超级账本与 IoT 和 IIoT 相融点

根据全球移动通信系统协会(GSMA)统计数据显示，2021 年全球物联网设备连接数量高达 147 亿个。物联网已经广泛地应用到众多领域，如前所述，区块链技术虽然被广泛研究但难以落地，物联网迫切地需要全新的技术解决所面临的挑战。本文总结了超级账本与物联网融合具备的基本优势：

a) 分布式存储和协作确保了大量数据和决策的抗篡改性。

b) 细粒度的权限控制增强了企业之间和消费者之间的隐私保护。

c) 细粒度的基于状态的背书策略加强了企业交易的安全。

d) 高效的共识机制有效地降低了设备或大型器械协作的网络延迟，并且能够更快地使节点状态达成一致，可以为工业物联网提供毫秒级的响应时间。

e) 点对点的身份认证确保了身份的高移植性，为便携式的物联网设备的身份识别提供了极大的便利。

f) 高度模块化的框架和支持多样化的链码编写语言使得超级账本能够快速与任何物联网和工业物联网系统集成。

g) 动态的网络使得系统具备强大的灵活性和健壮性，能够满足物联网基本的业务需求。

3　超级账本在物联网领域相关应用研究

在本节中，将物联网方向的研究细分为物联网安全、智能渔业和智能农业、智能玩具和 IoT 游戏、智能健身、智能城市监控、智慧交通、智能电网、智慧建筑项目和智慧能源(节能方向)9 个应用领域。

3.1　物联网安全领域

在当前的研究中，数据的隐私性、机密性和完整性安全比其他安全需求受到了更多的关注。由于物联网设备所产生的大量数据主要由集中式的云服务处理，这些数据很难保证其隐私性和机密性。Wang[7]提出了基于超级账本(Fabric 1.1.0)的物联网数据完整性验证方案。如图 1，将物联网数据分割为多个碎片，通过预先设定的智能合约(链码)实现自动验证和处理设备元数据，并存储记录。云服务提供商只负责将验证结果返回用户。减少了开销和计算成本，但缺少处理比较复杂的数据类型的设计。为解决不同云服务提供商之间的交易安全问题，Yang[8]提出了基于超级账本(Fabric 1.0)的联合云系统。该系统设计了通过用户信用值确定受信等级机制，代替了集中式管理，不同云服务提供商之间签署链码进行安全交易。在一定程度上保证信任，提高了云计算资源的利用率。在存储数据集的云服务中，存在数据所有者的数据集模型被恶意窜改和单点故障的风险，Dib[9]提出了基于超级账本(Fabric 1.1)的数据集利用系统。云服务只存储数据所有者加密的数据模型，消费者在共享数据集时通过超级账本进行付

费服务。增强了数据集被利用的透明度和数据集的安全性，但没有设计针对高信任级别用户的监管策略。为解决不同参与者之间的数据共享，于金刚[10]提出了一种基于超级账本(Fabric 1.4.0)的物联网数据共享模型。设计了新型网关实现收集数据、存储证书、身份验证以及数据格式清洗和转换。该模型确定了基于超级账本的物联网数据共享模型的关键组件，证实了超级账本能够提高物联网数据共享的效率。在供应链系统中，数据安全性是首先要考虑的问题，Cao[11]提出了一种钢材业的追溯系统(Sawtooth)。如图 2，通过智能合约将各个环节的数据进行存储，监管部门通过区块获取整个流通数据。消费者扫描 RFID 码获取最终的追溯信息。张森[12]提出一种冷链物流数据安全方案。如图 3，利用超级账本(Fabric)确保物流数据的实时上链，结合 Diffie-Hellman 密钥交换算法生成共享密钥确保用户的隐私性。

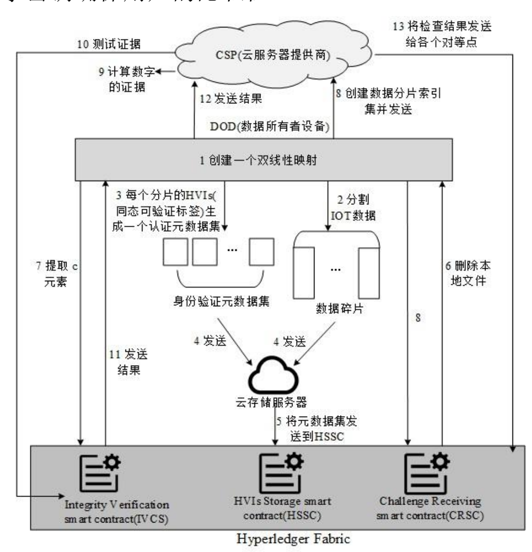


图 1　基于超级账本的物联网数据完整性验证方案的重构图

Fig. 1　Reconstruction diagram of a Hyperledger-based data integrity verification scheme for the iot

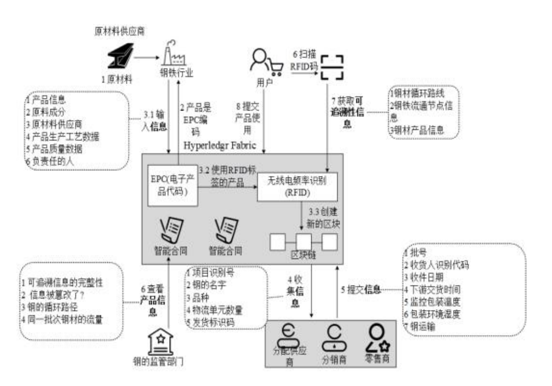


图 2　钢材业追溯系统的重构图

Fig. 2　Reconstruction diagram of traceability system in steel industry

被入侵设备的自动处理能够及时避免危险行为，Rodriguez[13]提出了基于超级账本(Fabric)的物联网设备监视方案。源设备与目标设备通过超级账本中背书节点验证交易可靠性，通过链码自动隔离危险设备。保证了设备数据的安全性。为解决延迟、效率等问题， Kim[14]提出了一个结合深度学习和超级账本(Fabric) 的轻量级方案。如图 4，系统根据网络节点的节点行为、经纬度等信息，使用聚类 K-Means 算法进行聚类并生成多个集群。系统生成对应的链验证器(由筛选的 4 个节点组成)验证通信合法性并存储交易记录。一定程度上提高了数据的安全性。物联网设备的配置数据是物联网数据的重要组成部分，一旦被窜改将直接影响原定的任务方向，Helebrandt[15]提出了基于超级账本(Composer)的物联网设备配置文件系统。如图 5，设计了链上和链外(存储大型配置文件)存储的方案，将修改配置的消息加密，并将管理 ID、设备 ID 和时间戳加载到新区块中。但缺少对更多配置信息的监管，比如电量、CPU 利用率和磁盘空间等。多级代理的方法有助于物联网数据的传输安全，Mbarekp[16]提出了基于超级账本(Fabric 1.1.0)的多级代理的物联网数据保护系统。如图 6，通过三级代理的检查验证区块的有效性，确保了数据的安全性。

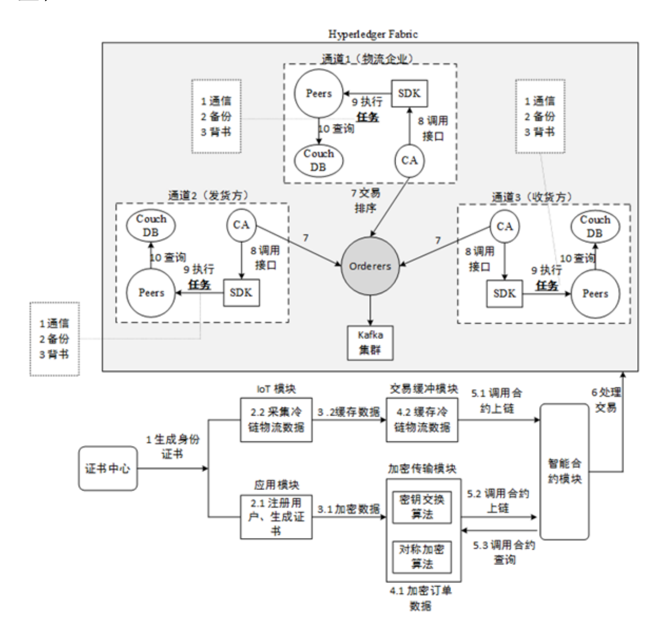


图 3　冷链物流数据安全方案的重构图

Fig. 3　Reconstruction diagram of the cold chain logistics data security scheme

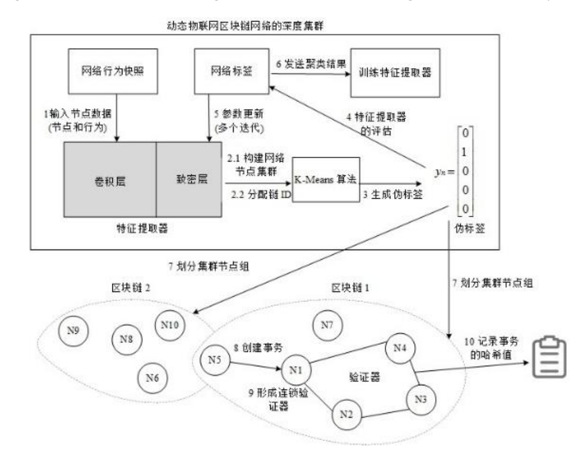


图 4　基于超级账本的轻量级方案的重构图

Fig. 4　Reconstruction diagram of a lightweight solution based on Hyperledger

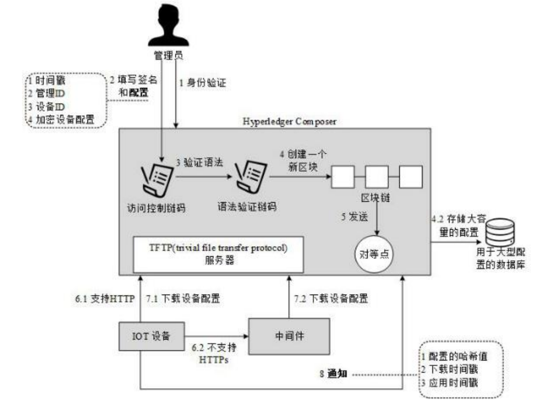


图 5　基于超级账本的物联网设备配置文件系统的重构图

Fig. 5　Reconstruction diagram of iot device configuration file system based on Hyperledger

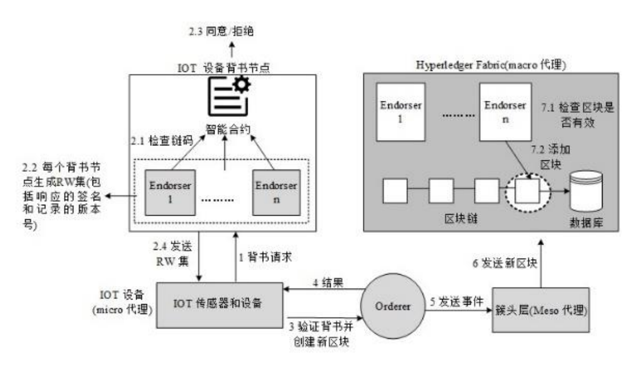


图 6　基于超级账本的多级代理的物联网数据保护系统的重构图

Fig. 6　Reconstruction diagram of iot data protection system based on Hyperledger with multi-level agents

由于超级账本中密钥管理大都由政府节点负责颁发和管理，仍存在密钥窜改、伪造等安全问题，Ribeiro[17]提出了分布式密钥管理的方案(Fabric 1.4.0)。通过设备与连接服务器签署智能合约，建立临时的会话密钥保障设备隐私，一定程度上解决了设备密钥的安全问题。

一些研究专注于物联网安全中身份验证、授权、计费等安全需求，Hang[18]提出了一个基于超级账本(Fabric 1.2)的物联网通信平台。如图 7，系统使用智能合约实现设备之间的安全访问，将数据存储于超级账本，提高了交易的安全性。由于其轻量级的架构，为实现大规模的物联网设备通信提供了可行性。为提高智能合约的可靠性，Liu[19]提出一种数据访问控制系统(Fabric 1.4.3)。多个用户共同制定访问控制策略，并通过超级账本存储记录和这些数据的 URL，减少了链上存储的压力。为解决顶级域名授权中的集中式根管理，Zhang[20]提出了基于超级账本(Fabric 1.4)的分布式根管理方案。如图 8，将某个域名授权的交易发送给多个授权节点，只有在时间阈值内响应的授权节点被认定为有效，并通过智能合约统计和自动处理授权消息。为提高身份验证的效率，Chi[21]提出了一种数据身份验证方案(Fabric)。如图 9，将用户的身份信息分割为标签数据和真实数据。根据 K-medoids algorithm[22]将网络划分多个社区，并利用 Cosine similarity 算法[23]衡量节点的标签数据与社区数据的相似性。用户根据标签检索相关信息。提高了身份相关数据检索和共享效率。张江徽[24]提出了一种基于超级账本(Fabirc 1.4.4)的访问控制策略模型。如图 10，利用智能合约实现细粒度的访问控制权限管理，在过度授权、越权访问的问题上具备较好的防御能力。

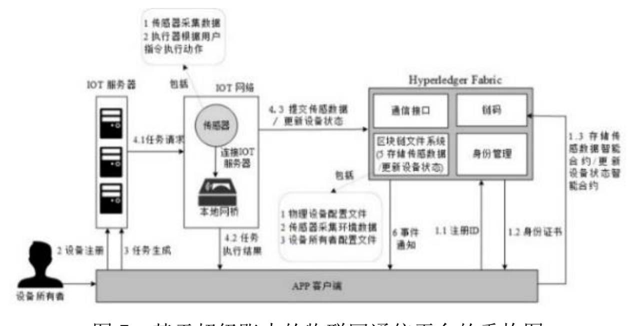


图 7　基于超级账本的物联网通信平台的重构图

Fig. 7　Reconstruction diagram of Hyperledger-based iot communication platform

在超级账本中，CA 的集中授权和认证可能会产生窜改、伪造等风险。为解决 CA 集中授权的问题，Siris[25]提出了基于超级账本(Fabric)的两种分散授权策略。如图 11，将多个组织授权代替了统一由 CA 节点授权，并根据节点的相应时间筛选某时刻交易的授权节点。在确保分布式授权安全性的同时提高了授权效率，但第一种策略需要更高的计算成本。为解决 CA 集中认证的问题，Kakei[26]提出了一种分布式的 CA 认证的策略(Fabric)。如图 12，将德克萨斯州的 CA 节点分为元 CA 和 CA。通过元 CA 与 CA 的交叉认证判断该 CA 节点是否为受信方，一定程度地提高了 CA 节点的可靠性。

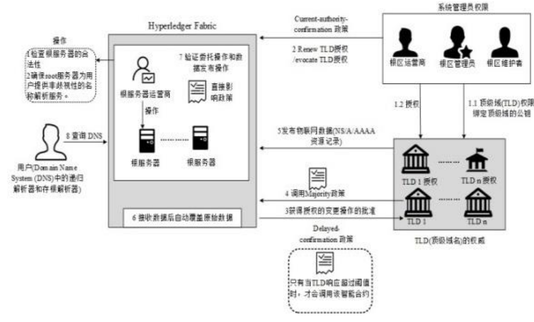


图 8　基于超级账本的分布式根管理方案的重构图

Fig. 8　Reconstruction diagram of a distributed root management solution based on Hyperledger

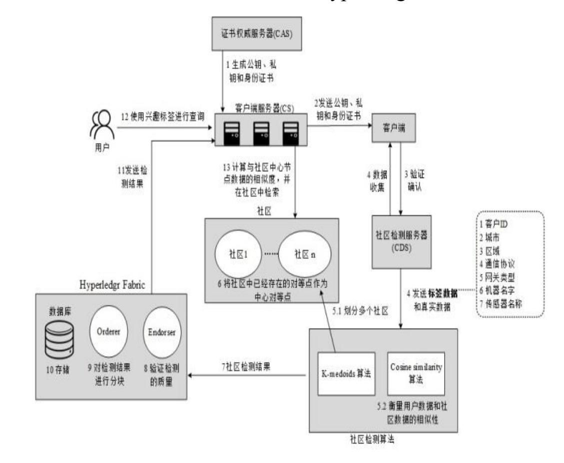


图 9　数据身份验证方案的重构图

Fig. 9　Reconstruction diagram of the data authentication scheme

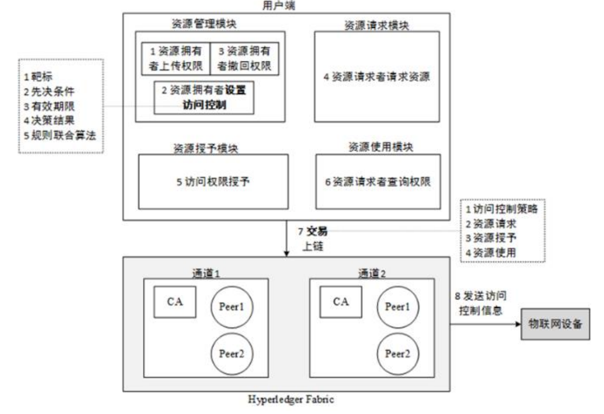


图 10　基于超级账本的访问控制策略模型的重构图

Fig. 10　Reconstruction diagram of the Hyperledger-based access control policy model

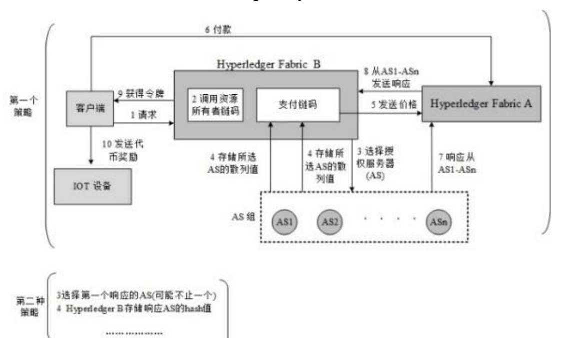


图 11　基于超级账本的两种分散授权策略的重构图

Fig. 11　Reconstruction diagram of two decentralized authorization strategies based on Hyperledger

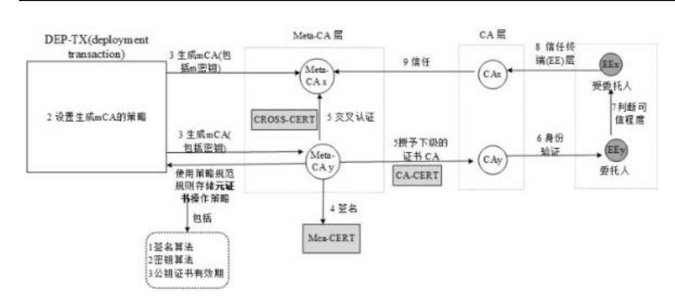


图 12　分布式 CA 认证策略的重构图

Fig. 12　Reconstruction diagram of distributed CA authentication policy

为提供一种通用型的基于超级账本的授权架构，Pajooh[27]提出了一种基于蜂窝系统的多层区块链模型(fabric)。如图 13，根据 SI (swarm intelligence)和 EC (Evolutionary computation)算法将网络分为三层，并在超级账本中连接多个基站，实现物联网设备的分布式授权和认证。该模型降低了网络负载，但是没有实际地搭建测试平台。

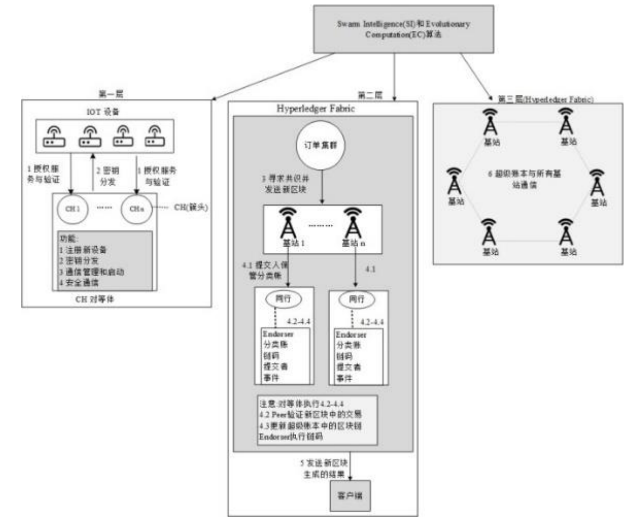


图 13　基于蜂窝系统的多层区块链模型的重构图

Fig. 13　Reconstruction diagram of a multilayer blockchain model based on a cellular system

基于超级账本开发的物联网系统应当满足服务可用性的安全需求，对数据加密是确保数据不被攻击的有效方式之一。Zhou[28]提出一种全同态计算的物联网数据保护方案(Fabric)。通过使用同态加密算法加密会话消息，并通过多个服务器验证消息是否被更改。有效地保护了物联网数据不被攻击，并具有良好的性能。Hou[29]提出了边缘计算保护数据的方案。如图 14，将设备的消息通过 LoRa 网关获取，并将上行消息存储在超级账本中，降低了消息被攻击的可能性。

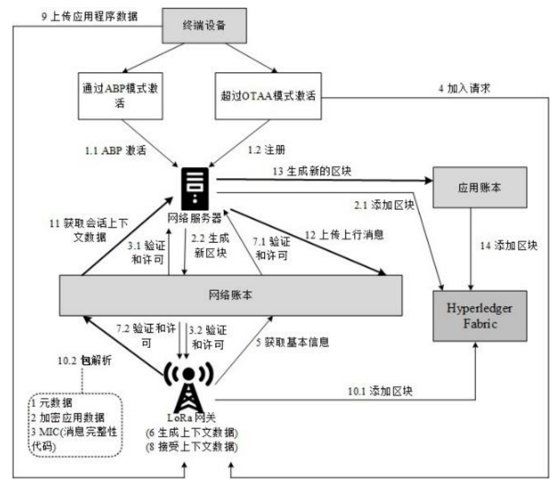


图 14　边缘计算保护数据方案的重构图

Fig. 14　Reconstruction diagram for edge computing protection data solution

3.2　智能渔业与智能农业领域

信息技术的进步促进了渔业和农业的数字化转型。在概念层面，智能渔业与智能农业相似。二者都是通过深度融合大数据、区块链、人工智能等信息技术，获取数据的实时采集、定量决策、智能控制、精准投资、产量预测、以及其他个性化服务[30]。智能渔业以水质监控为主，实现大面积水质的分析和调控。相比之下，智能农业的主要需求是通过实时监控和分析进行智能决策，以提高生产力和资源效率[31]。目前，超级账本在智能渔业和农业的应用较少，解决的问题主要集中在数据的抗窜改性和实时数据流。

渔场的准确调控和数据不被窜改具有一定难度。Hang[32]提出了基于超级账本(Fabric 1.4.3)的智能养鱼平台。如图 15，通过水位传感器预测实际水位数据，利用 Kalman filter 算法消除误差，并计算实际所需的水位和持续时间，进行自动调控。该平台为智能渔业提供了更安全的开发思路，但是缺少与不同渔场的交互。

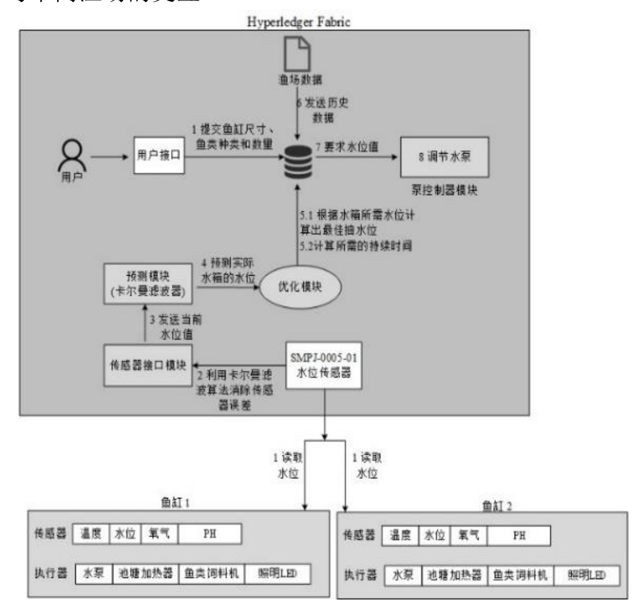


图 15　基于超级账本的智能养鱼平台的重构图

Fig. 15　Reconstruction diagram of smart fish farming platform based on Hyperledger

在智能农场系统中，有关农作物的实时监测以及监测产品数据的可靠性问题，Lee[33]提出了基于超级账本(Sawtooth)的食品生长环境监测的中间件。如图 16，将传感器收集的农作物数据上链，超级账本对监测数据执行 10 个周期的认证。证明了 POET(Proof of Elapsed Time)共识具有更快的处理效率，具备实际适用性。为解决查询追溯信息时间过长问题，弋伟国[34]提出了一种基于超级账本(Fabric 2.0)的增强果蔬产品追溯可信度系统。如图 17，通过数据哈希值二次上链和验证改进了“数据入库+哈希值上链”的数据保存、提前验证并上链和追溯方面的性能。降低了查询时间算法的复杂度。

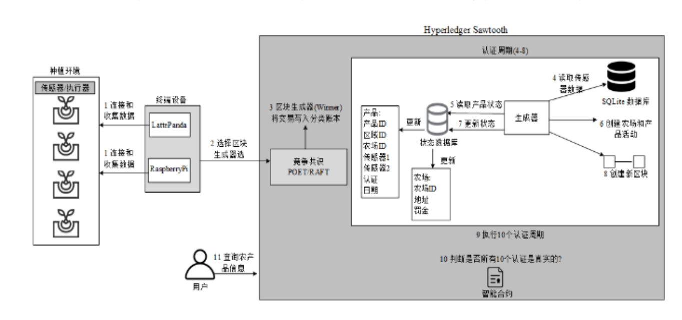


图 16　基于超级账本的食品生长环境监测中间件的重构图

Fig. 16　Reconstruction diagram of the middleware for food growth environment monitoring based on Hyperledger

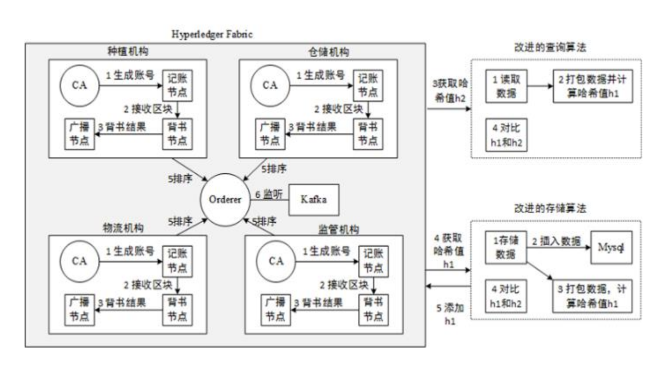


图 17　基于超级账本的增强果蔬产品追溯可信度系统的重构图

Fig. 17　Reconstruction diagram of Hyperledger-based system for enhancing the trustworthiness of fruit and vegetable product traceability

3.3　智能玩具和 IoT 游戏领域

智能玩具与 IoT 游戏虽然都属于智能化的娱乐服务，但实现的目标却大相径庭。智能玩具的用户主要由儿童组成，通过融合 IT 技术实现打电话、儿童教育、浏览网站、位置追踪和其他服务。全球市场上的智能玩具类型包括附加机械玩具、声音/图像识别玩具、无屏幕玩具、生活玩具、益智和建筑玩具，以及健康跟踪/可穿戴玩具[35]。然而智能玩具面临横向数据无法交换的问题。这是由于异构的 APIs 很难完成不同系统间的数据交换[35]，导致大量的冗余数据(用户不需要的数据)无法得到有效利用。IoT 游戏突破了以图像和视频为主的传统意义，是一种以物联网技术为主要动力，在物理世界的真实物体之间进行互动获取奖励的游戏。因此，IoT 游戏面向的对象是分散的，主要包括基于位置的感知游戏。然而这种游戏缺少一个强大的技术保证任务的真实性和用户的隐私不被侵犯。超级账本为上述问题的解决提供了有效的解决方法。

在智能玩具的数据共享中，横向的数据安全交换具有一定难度，Yang[36]提出了基于超级账本(Fabric 1.0)的玩具数据交换模型。如图 18，玩具数据经过脱敏处理后供应商为玩具生成唯一标识，超级账本将玩具数据检查并存储于 Couch DB，以确保存储安全。

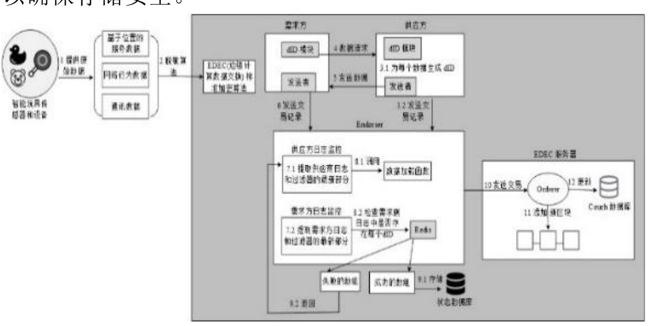


图 18　基于超级账本的玩具数据交换模型的重构图

Fig. 18　Reconstruction diagram of the Hyperledger-based toy data exchange model

在基于超级账本的 IoT 游戏系统中，有关游戏任务的实时更新、玩家隐私以及游戏任务位置的可靠性问题，Manzoor[37]提出了基于位置感知的移动狩猎游戏(Fabric)。玩家所提交的狩猎任务通过智能合约进验证，并只发布奖励信息，不显示狩猎细节。通过钱包功能确保玩家的奖励，将完成的任务信息存储在超级账本中。增强了基于位置游戏的奖励透明度和安全性，但是物联网信标的检测延迟较大，并且无法保证狩猎的位置是安全的。考虑到部分玩家无法完成狩猎任务的情况，Pittaras[38]开发了以太坊和超级账本(Fabric 1.4)互连的基于位置的移动游戏(由于原文没有说明以太坊的设计，图中只展示超级账本相关的设计)。开发了广告功能，并利用链码统计玩家观看广告的次数和自动发放奖励。

3.4　智能健身领域

智能健身是物联网领域的热门场景之一。智能健身旨在通过传感器获取用户的训练数据，再结合人工智能算法提供智能训练决策、监督饮食、预测行为等服务。基于物联网的智能健身分为三类：健身追踪器(包括可穿戴和非可穿戴传感器)、运动分析和健身应用[39]。目前，超级账本主要为智能健身解决了训练模型以及决策的安全、并增强了精准的自动化服务。

基于超级账本的健身数据系统中，为提供更安全的智能服务，Jamil[40]提出了一个基于超级账本(Fabric 1.2，Composer 1.13.0)的健身模型。如图 19，利用机器学习实现健身数据的推理引擎，提供合理的健身计划和饮食计划。并将推理知识的阈值与实际读取的数据进行比较和存储，更新推理信息。提高了健身数据的安全性。

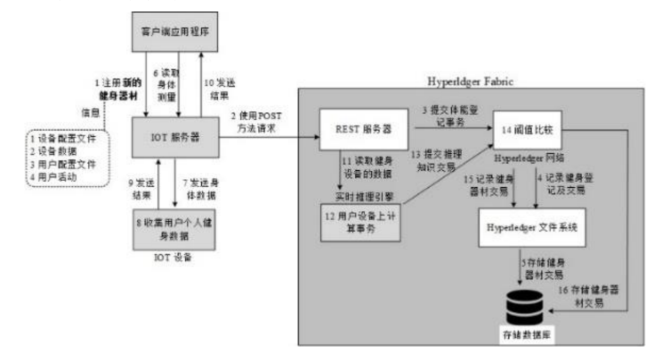


图 19　基于超级账本的健身模型的重构图

Fig. 19　Reconstruction diagram of the fitness model based on Hyperledger

3.5　智能城市监控领域

城市监控是智能城市中重要的基础设施。基于物联网的城市监控是通过摄像机收集信息以获取地理空间的实时状态，并对这些数据进行智能化的分析和检测。

城市监控系统中，有关用户提供的监控信息真实性的问题，Khan[41]提出了基于超级账本的监控信息检测系统。如图 20，通过超级账本(Fabric 1.4)的背书节点判断监控视频/图像的重要性，利用链码将重要的信息优先检测并提取帧数与原视频比较。该系统在一定程度上确保了 CCTV(Closed-Circuit Television Camera)数据的真实性，但是检测机制单一。

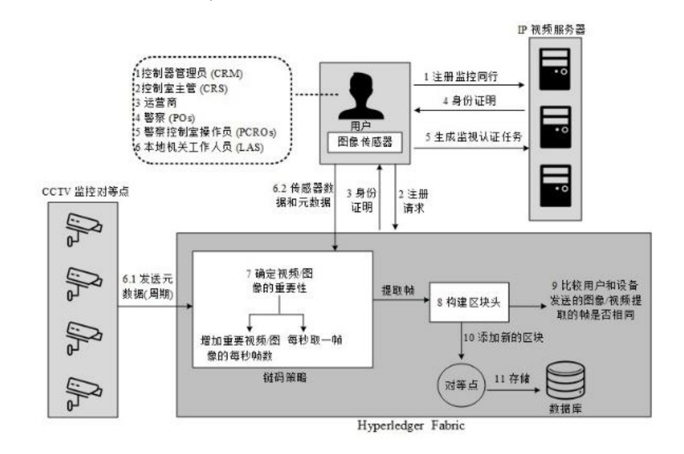


图 20　基于超级账本的监控信息检测系统的重构图

Fig. 20　Reconstruction diagram of Hyperledger-based monitoring information detection system

3.6　智能电网

智能电网是一种先进的数字双向潮流电力系统，具有自愈、自适应、弹性和可持续性，并能对不确定性进行预测[42]。智能电网对可靠的，可持续的电力供应具有较高的要求[43]，安全的电力双向交易是确保可持续供应的重要因素。安全除

了安全存储、交易可追踪之外，还包括合理的隐私保护。目前基于超级账本的研究主要集中在解决电力交易、隐私保护以及能耗负载。

在基于超级账本的智能电网系统中，实时调度策略是电力交易的重要部分。Zhao[44]建立了基于超级账本(Fabric 1.1)的微电网市场模型。利用多个链码对电力资源进行实时调度，将交易记录存储于超级账本区块链上。并根据不完全信息静态博弈的贝叶斯-纳什均衡理论确定交易价格和交易量，有效地降低了电力用户的购买成本，但是无法保证在处理大量的交易时的系统性。Li[45]提出了基于超级账本(Fabric 1.4.0)的双向电力交易系统。如图 21，通过基于迭代双层优化的充放电策略为电动车制定实时调度策略，并利用链码进行调度交易和清算。分层电力调度的结构有助于提高系统的可扩展性。考虑到交易的稳定性，Li[46]提出了一种电力调度方案(Fabric 1.4.0)。如图 22，根据改进的磷虾群算法的优化模型对电动汽车的充/放电制定了充/放电时间表，将电网的负荷方差最小化，进而提高了电动汽车的电力交易的安全性和稳定性。在电力交易中，合理的出价策略有助于电力调度，Yu[47]提出了基于超级账本(Fabric)的电力交易模型。通过改进贝叶斯竞价算法为用户提供最佳出价策略，包括可能的出价类型、最佳出价和对手的概率分布。并采用用户层，代理层和超级账本层的三层结构确保详细的交易信息不会被代理和超级账本获取。为解决用户由于过度调度导致的供应链失衡，Lohachab[48]讨论了一种新型的电能交易框架(Fabric 1.4.0, Fabric 1.4.1)。将超级账本实时调度代替集中式的微电网调度电能，并设计了奖励算法和调度算法鼓励用户出售多余电能、维持电能的需求平衡和保证每个用户的能量水平在最低需求和最大需求之间。提高电能的利用率。

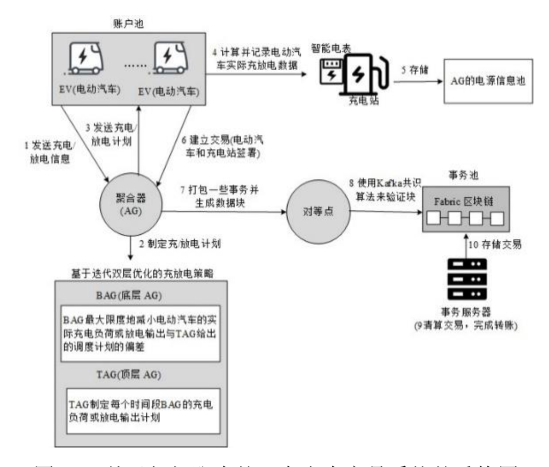


图 21　基于超级账本的双向电力交易系统的重构图

Fig. 21　Reconstruction diagram of a two-way power trading system based on Hyperledger

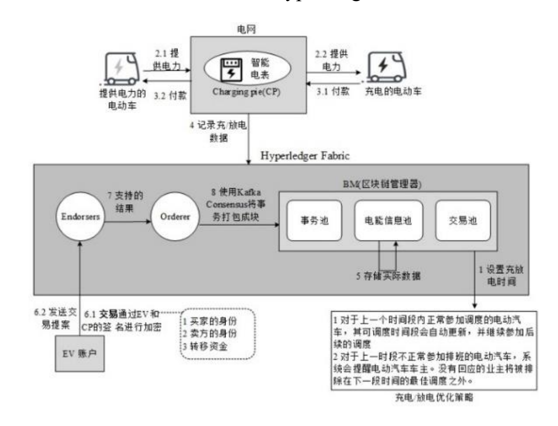


图 22　电力调度方案的重构图

Fig. 22　Reconstruction diagram of the power dispatch scheme

为保证不同时期能源交易的稳定性，Jamil[49]结合机器学习和超级账本(Fabric 1.2)，提出了一种智能电力交易平台。如图 23，根据物理网络收集客户信息，利用机器学习分析数据特征并预测短期和长期的调度交易。有效地保证了网络负载，但预测的指标单一。为更好的缓解电力系统峰值时的网络拥塞，众包任务是有效的方案，Sciume[50]提出一种能耗负载响应方案(Fabric)。通过数据集线器预测第二天的网络负载，将降低网络负载任务众包给用户。利用智能合约根据基线评估每个参与降低电力网络负载的用户的实际负载能力，并分配相应的奖励任务，有效地解决了电力系统中峰值负载造成的网络拥塞。在智能电力交易中，关于用户隐私保护，Wang[51]提出了一个电能管理系统。采用实体映射协议均值和零知识证明相结合的认证方法来分离用户信息，保证用户的隐私。

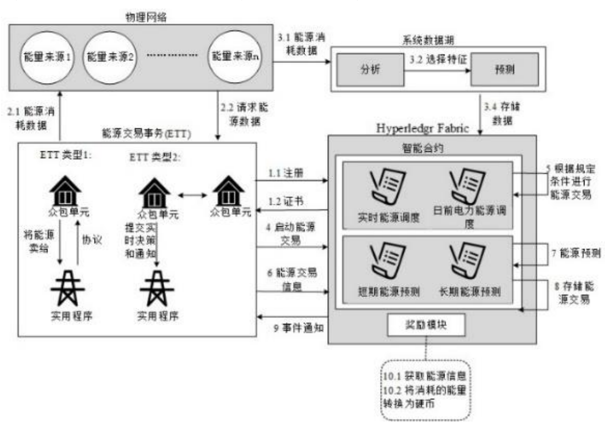


图 23　智能电力交易平台的重构图

Fig. 23　Reconstruction diagram of the smart power trading platform

3.7　智慧交通

智慧交通是利用人工智能的潜力，开发大数据驱动的智慧交通管理解决方案，实现有效决策[52]。这种决策大部分是指有效地避免或减缓交通拥堵和交通事故[53]。在面对高流动性、高动态性的交通情况时作出快速且精准的调控成为了急需解决的挑战。目前，超级账本在智慧交通的研究覆盖了多个方面，包括自动认证、交叉口调控与监控、ETC(Electronic Toll Collection)、空陆一体化认证和车联网数据安全。

在基于超级账本的车辆系统中，有关实时身份认证的问题，Feng[54]提出了一种基于超级账本(Fabric,Composer 0.20.7)的自动认证车辆信息系统。如图 24，将车载单元作为车辆的唯一身份标识，利用路边单元和车载单元进行实时检测，并通过链码自动认证。其中，车辆的身份在认证过程中被加密，提高了认证的隐私性。

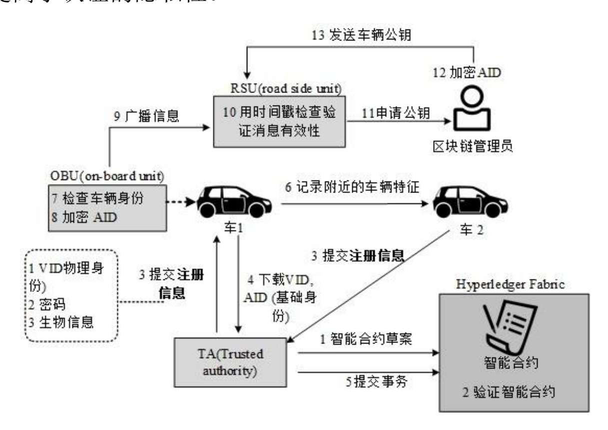


图 24　基于超级账本的自动认证车辆信息系统的重构图

Fig. 24　Reconstruction diagram of automatic certified vehicle information system based on Hyperledger

为解决跨域身份认证，Li[55]提出了基于超级账本(Fabric 1.2，Ursa)的车辆位置感知系统。如图 25，采用 I-SIG 系统获

取车辆的数据，为交叉路口提供最优的信号方案，并使用零知识范围证明(Zero Knowledge Range Proofs，ZKPR)协议加密车辆的信息，最后通过智能网关核实车辆身份的合法性。在交易延迟、吞吐量和成功率上具有较好的优势。由于路边单元的监测范围有限，一些方案致力于结合空中资源进行监测，Luo[56]提出了空陆一体化的车辆跨域身份监控系统(Indy)。如图 26，利用软件无线电设备(Universal Software Radio Peripheral，USRP)技术提供车辆的身份特征，通过无人机对车辆身份进行认证，并采用相邻无人机交叉认证的方式确保无人机的身份的合法性。利用空中节点扩大了监测范围，但认证的延迟较高。

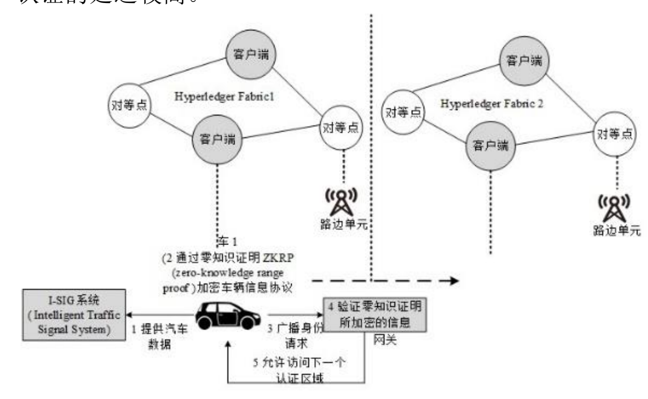


图 25　基于超级账本的车辆位置感知系统的重构图

Fig. 25　Reconstruction diagram of a Hyperledger-based vehicle location-aware system

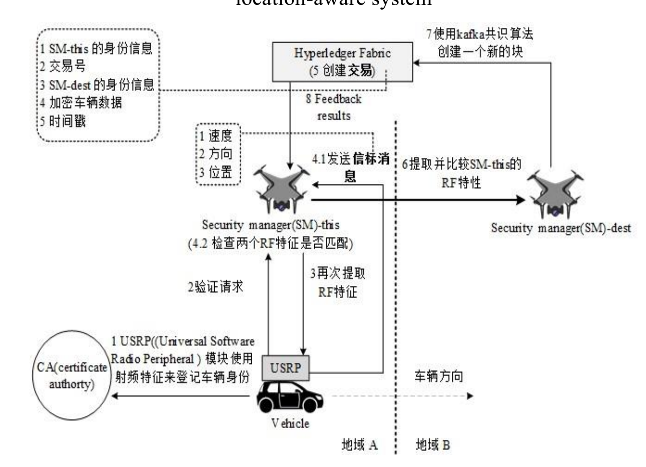


图 26　空陆一体化的车辆跨域身份监控系统的重构图

Fig. 26　Reconstruction diagram of an air-land integrated vehicle cross-domain identity monitoring system

针对交叉路口的交通安全问题，Buzachis[57]提出了基于超级账本(Fabric)的监控交叉路口的车辆系统。通过链码对车辆进行实时的轨迹仿真，背书节点负责检测仿真结果。测试了在 1-2 个路口的自动驾驶汽车通过交叉口的情况，证明该系统的可用性，但是没有针对多个交叉路口的设计。为解决车辆发生危险实时协助问题，Mbarek[58]提出了一种多级背书的车辆通信系统(Fabric)。利用 BF-DF-AF-IF(Belief function-Desire function -Analysis function -Intension function)模型将车辆的需求细化为具体的修理行动需求。设计背书等级机制(根据交易所获得的分数，由链码自动升级或降级背书等级)，将每笔交易由更高等级的背书节点进行背书，确保交易的可靠性。实现了智能化的背书机制，增强了背书效率，但评分机制不够完整。针对车联网中事故信息的真实性，Xiao[59]提出了一种车联网假新闻检测模型(Fabric)。如图 27，采用贝叶斯算法检测车联网消息真实性的概率并存储在超级账本中。实现了负载均衡，并在先验概率、事务处理速度和准确性方面证明其可行性。为能及时获取路面情况，避免交通事故，Chen[60]提出了一种基于边缘服务器的车辆区域信息拍卖方案。如图 28，利用边缘服务器划分地区，并发布某地区信息报告的请求任务。通过路边单元(Road Side Unit，RSU)技术将完成任务的车辆进行身份识别，并利用最大期望算法(Expectation maximization，EM)算法评估信息的真实性。适用于低功耗设备，确保了数据的质量和奖励。

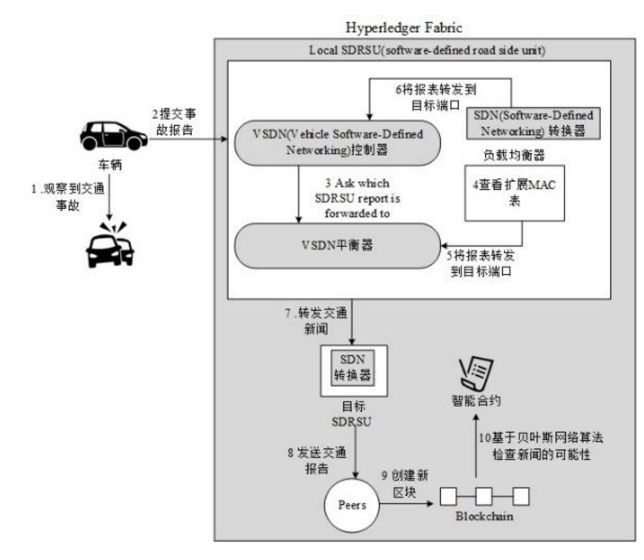


图 27　车联网假新闻检测模型的重构图

Fig. 27　Reconstruction diagram of a fake news detection model for Telematics

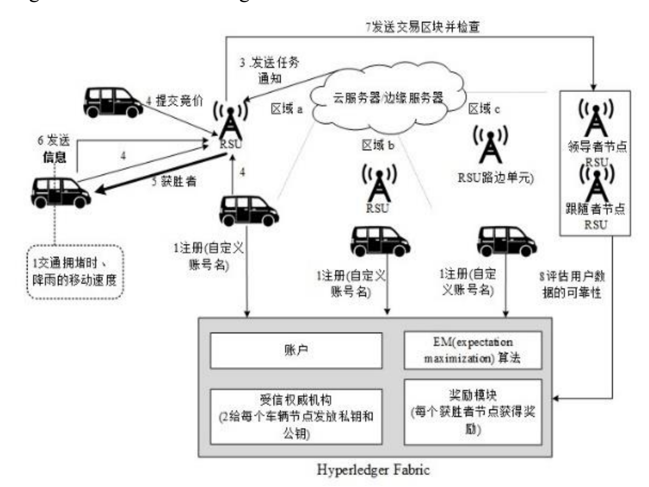


图 28　基于边缘服务器的车辆区域信息拍卖方案的重构图

Fig. 28　Reconstruction diagram of the edge server-based vehicle area information auction scheme

一些研究致力于智慧交通中安全交易问题。Gao[61]提出了基于超级账本(Fabric 0.6)的 V2G(Vehicle-to-grid)支付模型。通过付款人在同一交易中可创建多个账户确保隐私。Chiu[62]提出了基于超级账本(Fabric 2.2)的 ETC 系统。车辆与 ETC 门进行交叉认证，由 ETC 门检测车辆的身份合法性，将交易记录存储于超级账本中。具有稳定性和高性能，但是 PBFT 共识并不适用于大型网络。在收费站系统中，为解决电子身份的问题，Viera[63]提出了一种基于 5G 的 C-V2X(Vehicle to Everything)的道路收费系统(Fabric)。如图 29，采用 Indy 的可移植身份技术，通过智能手机发送身份信息代替路边单元获取身份信息。通过手机处理收费请求并存储交易记录。该提案首次在 V2X 系统中展示了 5G 与超级账本结合的可行性。Lee[64]提出了一种基于拍卖机制和雾计算的交通系统(Fabric)。如图 30 所示，利用雾计算将公共交通资源进行分配，并设计了拍卖机制选择出价最高的车联网用户。实现了公共交通资源的合理分配，但选择获胜者的方式单一。另外，相邻 RSU 节点默认是安全的，降低了背书结果的可信度。

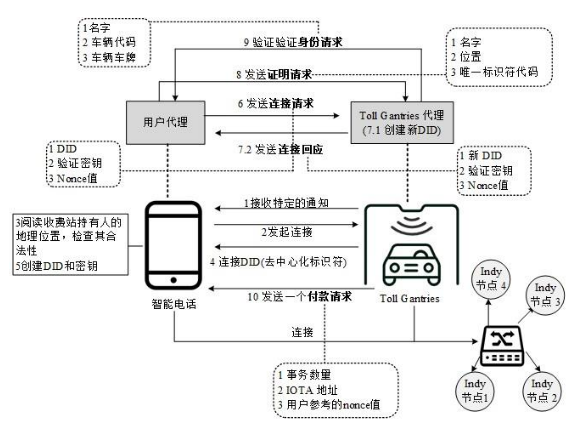


图 29　基于 5G 的 C-V2X 道路收费系统的重构图

Fig. 29　Reconstruction diagram of 5G-based C-V2X road tolling system

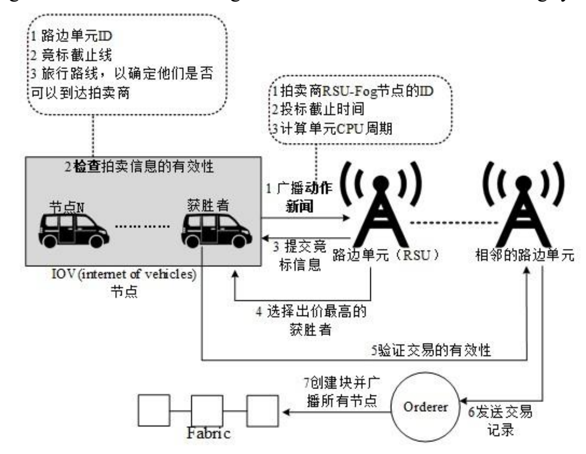


图 30　基于拍卖机制和雾计算的交通系统的重构图

Fig. 30　Reconstruction diagram of the traffic system based on auction mechanism and fog computing

3.8　智慧建筑项目

在本文中，智慧建筑项目是指将建筑项目和前沿的 IT 技术高度融合，以达到实时更新建筑建模、交易安全、降低交付成本、有效协作的目的[65, 66]。目前的研究大多集中在解决建筑类项目中多方信息交换。

针对建筑项目信息交换的问题，Suliyanti[67]提出了一种多个相关方交换建筑信息的系统(Fabric，Composter)。如图 31，系统开发了建筑项目竞标系统，并将建筑完成的整个周期存储于超级账本。探索了建筑信息模型(Building Information Modeling，BIM)信息的完整记录和交换，但是该方案过于以业主为中心，导致业主的选择没有适当的监管方式。针对建筑项目中财务分配问题，Elghaish[68]提出了一种建筑信息模型系统(Fabric)。如图 32，利用智能合约检查施工团队的财务分配，根据总利润、成本节约和已偿还成本的净金额向每个参与者分配相应的财务。该方案证明了超级账本应用于集成项目交付(Integrated Project Delivery，IPD)系统的可行性。为解决不同建筑项目账本隐私性问题，Yang[69]讨论了一个多通道的设计方案(Fabric)。如图 33，通过智能合约实现架构师与供应商、工程师、客户端、建筑测量师和城市规划师之间的通信，并将每一个环节的信息存储在不同通道中。这项研究确定了基于超级账本的建筑项目系统在可扩展性、跟踪性和可审计性特征上独有的优势，和在事务处理效率、业务变动、身份、成本和智能合约的安全性等方面的挑战。针对建筑项目信息不完整问题，Sheng[70]提出了一种基于超级账本(Fabric 1.4)的建筑项目信息管理系统。系统通过超级账本的背书节点检查建筑信息的真实性、利用 Orderer 进交易排序，通过 Web 查询完整的建筑项目信息。在一定程度上解决了建筑项目信息的不完整性和难追溯问题。

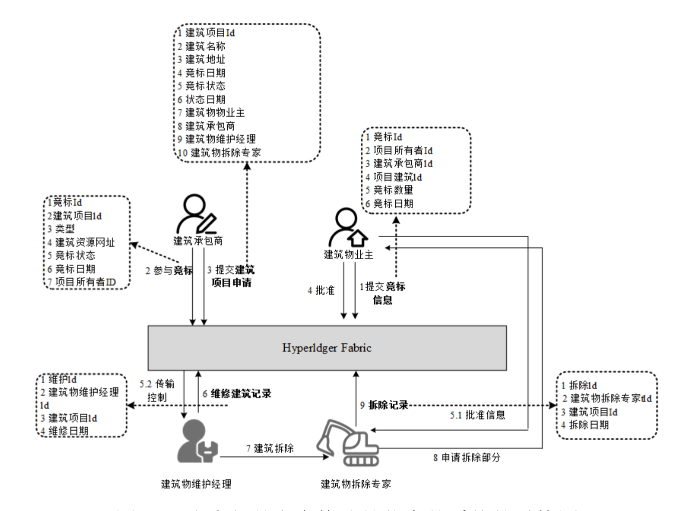


图 31　多个相关方交换建筑信息的系统的重构图

Fig. 31　Reconfiguration diagram of a system for multiple interested parties to exchange building information

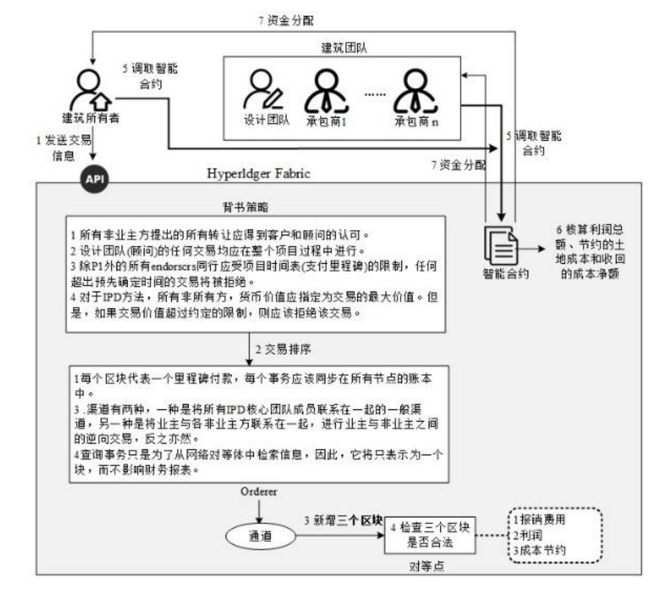


图 32　建筑信息模型系统的重构图

Fig. 32　Reconstruction diagram of building information model system

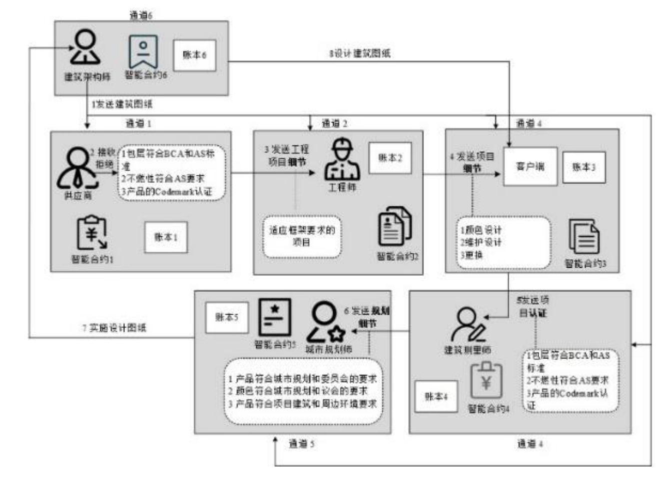


图 33　多通道的设计方案的重构图

Fig. 33　Reconstruction diagram of a multi-channel design solution

3.9　智慧能源

智慧能源交易旨在通过消费者和企业之间出售自己剩余能源或购买自己所需能源，实现自主能源调控和有效的能源利用。在本节中能源的概念可能是电能或碳排放量。智慧能源交易提高了能源的利用率，减少了人工的误差和管理成本。超级账本主要解决了智慧能源交易中安全交易、交易完整性

验证的问题。

为解决能源排放的安全调度，Yuan[71]提出了基于超级账本(Fabric 1.1)的能源排放交易系统。节点通过特定通道分配排放量，利用智能合约对能源排放交易进行存储和审查。为确保能源排放量交易身份的合法性，Hu[72]提出了分布式能源交易的模型(Fabric)。通过背书节点验证企业的身份和所申请的排放量，并将交易信息存储于链上。为提高能源排放交易的验证效率，Che[73]提出了在链上和链外共同验证能源交易的方案(Fabric 1.1)。如图 34，由匹配单元打包并验证一定数量交易，再由链上对等点再次验证并存储。为提高能源的调度效率，Silva[74]提出了电动车能源竞标系统。利用超级账本(Fabric，Composter)设计了竞标电能，并连接本地停车场的控制器进行电能调度。利用链码完成电能交易，在交易的完整性和透明度具有较好的优势，但是买方在交易中接近中心化，监管买方存在明显的不足。

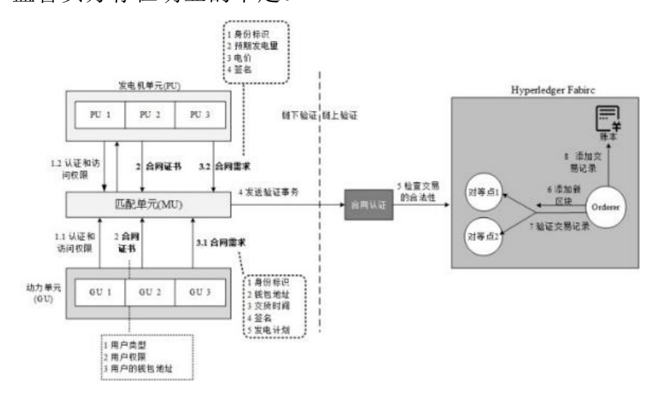


图 34 链上和链外共同验证能源交易的方案的重构图

Fig. 34 Reconstruction diagram of the scheme for on-chain and off-chain co-validation of energy transactions

4 未来研究方向

随着超级账本技术的应用和研究，物联网与超级账本融合引起了广泛关注。超级账本解决了其他区块链技术在灵活性、健壮性和隐私性等方面的不足，但是基于超级账本的物联网系统仍然存在一些问题没有充分研究和解决，这些局限性主要集中在性能和激励机制方面。为此，本文提出了四个未来方向：

a) 低能耗共识算法。共识算法是决定基于超级账本的物联网系统性能的关键因素。大部分的物联网设备无法完全满足处理大量共识时所需的计算和高能源。因此，适用于大部分物联网设备的低能耗共识算法是一项急需解决的重要问题。

b) 智能交易验证。超级账本中的“Endorse+Kafka+Commit”等模式并没有完全解决交易验证的性能问题，现有的交易验证性能仍然无法满足处理大量物联网设备之间的信息交换需求。某些参与验证的节点响应时间过长将影响交易验证的效率。因此，利用一些智能聚类算法筛选当前活跃度较高的节点承担验证角色可能会解决此问题[12]。

c) 链上链下混合存储。超级账本的区块存储于节点中，然而这些节点通常是物联网设备。某些设备存储容量很低，无法存储多条区块链。利用一些分布式数据库(如 IPFS 等)与超级账本融合进行链上链下存储可能会缓解设备的存储压力。

d) 自定义激励机制。超级账本不提倡任何的加密货币作为奖励，但是分布式的任务承担仍然需要激励机制作为主要驱动力。本研究认为这种激励机制可以是自定义的，开发者可以重点关注消费者的兴趣领域。比如，消费者对某种游戏或某网站的会员服务情有独钟，那么该消费者的任务奖励可以在这些选项中自行选择。这种激励机制将提高协作效率，激励用户更好的参与协作。

5 结束语

基于区块链开发的物联网系统在可扩展性、灵活性、健壮性和隐私性方面存在明显的不足。为解决上述问题，超级账本被视为一种理想的技术并引起了广泛的关注。本研究归纳并总结了超级账本在物联网的研究，展示了超级账本在物联网中应用的可行性和有效性。旨在以重构图视角展示更直观的差异和设计思路，为研究人员提供快速的技术融合指南。超级账本技术已能够满足多种业务场景，但在物联网领域的探索还在初步阶段。此外，重构图的综述方式在可视化的业务逻辑、技术融合、易读易懂等方面初步体现出独特的优势。

参考文献：

[1] Khan M A, Salah K. IoT security: Review, blockchain solutions, and open challenges [J]. Future generation computer systems, 2018, 82: 395-411.

[2] Blummer T, Sean M, Cachin C. An introduction to hyperledger [J]. Hyperledger Organization: San Francisco, CA, USA, 2018. https://www. hyperledger. org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger. pdf.

[3] Leng Zeqi, Tan Zhenjiang, Wang Kunhao. Application of Hyperledger in the Hospital Information Systems: A Survey [J]. IEEE Access, 2021, 9: 128965-128987.

[4] Keramidas G, Voros N, Hübner M. Components and Services for IoT Platforms [M]. Cham: Springer International Pu, 2016.

[5] Olson K, Bowman M, Mitchell J, *et al.* Sawtooth: an introduction [J]. The Linux Foundation, Jan, 2018: 26. https://www. hyperledger. org/wp-content/uploads/2018/01/Hyperledger_Sawtooth_WhitePaper. pdf.

[6] LEE I, LEE K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises [J]. Business Horizons, 2015, 58 (4): 431-40.

[7] Wang Haiyan, Zhang Jiawei. Blockchain based data integrity verification for large-scale IoT data [J]. IEEE Access, 2019, 7: 164996-165006.

[8] Yang Hui, Yuan Jiaqi, Yao Haipeng, *et al.* Blockchain-based hierarchical trust networking for JointCloud [J]. IEEE Internet of Things Journal, 2019, 7 (3): 1667-1677.

[9] O Dib O, Huyart C, Toumi K. A novel data exploitation framework based on blockchain [J]. Pervasive and Mobile Computing, 2020, 61: 101104.

[10] 于金刚, 张弘, 李姝, 毛立爽, 姬鹏翔. 基于区块链的物联网数据共享模型 [J]. 小型微型计算机系统, 2019, 40 (11): 2324-2329. (Yu Jin-gang, ZhangHong, Li Shu, Mao Li-shuang, Ji peng-xiang. Data Sharing Model for Internet of Things Based on Blockchain [J]. Journal of Chinese Computer Systems, 2019, 40 (11): 2324-2329.)

[11] Cao Yan, Jia Feng, Manogaran G. Efficient traceability systems of steel products using blockchain-based industrial Internet of Things [J]. IEEE Transactions on Industrial Informatics, 2019, 16 (9): 6004-6012.

[12] 张森, 叶剑, 李国刚. 面向冷链物流的区块链技术方案研究与实现 [J]. 计算机工程与应用, 2020, 56 (03): 19-27. (Zhang Sen, Ye Jian, Li Guogang Research and Implementation of Blockchain Technology Scheme for Cold Chain Logistics [J]. Computer Engineering and Applications, 2020, 56 (03): 19-27.)

[13] Seshadri S S, Rodriguez D, Subedi M, *et al.* IoTcop: A blockchain-based monitoring framework for detection and isolation of malicious devices in internet-of-things systems [J]. IEEE Internet of Things Journal, 2020, 8 (5): 3346-3359.

[14] Kim J H, Lee S, Hong S. Autonomous Operation Control of IoT Blockchain Networks [J]. Electronics, 2021, 10 (2): 204.

[15] Košťál K, Helebrandt P, Belluš M, *et al.* Management and monitoring of IoT devices using blockchain [J]. Sensors, 2019, 19 (4): 856.

[16] Mbarek B, Jabeur N, Pitner T. Mbs: Multilevel blockchain system for IoT [J]. Personal and Ubiquitous Computing, 2019: 1-8.

[17] V Ribeiro V, Holanda R, Ramos A, *et al.* Enhancing key management in LoRaWAN with permissioned blockchain [J]. Sensors, 2020, 20 (11): 3068.

[18] Hang Lei, Kim D H. Design and implementation of an integrated IoT blockchain platform for sensing data integrity [J]. Sensors, 2019, 19 (10): 2228.

[19] Liu Han, Han Dezhi, Li Dun. Fabric-IoT: A blockchain-based access control system in IoT [J]. IEEE Access, 2020, 8: 18207-18218.

[20] Zhang Yu, Liu Wenfeng, Xia Zhongda, *et al.* Blockchain-Based DNS Root Zone Management Decentralization for Internet of Things [J]. Wireless Communications and Mobile Computing, 2021, 2021.

[21] Chi Jiancheng, Li Yu, Huang Jing, *et al.* A secure and efficient data sharing scheme based on blockchain in industrial Internet of Things [J]. Journal of Network and Computer Applications, 2020, 167: 102710.

[22] Yu Donghua, Liu Guojun, Guo Maozu, *et al.* An improved K-medoids algorithm based on step increasing and optimizing medoids [J]. Expert Systems with Applications, 2018, 92: 464-473.

[23] Fauzi M A, Utomo D C, Setiawan B D, *et al.* Automatic essay scoring system using n-gram and cosine similarity for gamification based e-learning [C]. Proceedings of the International Conference on Advances in Image Processing. 2017: 151-155.

[24] 张江徽，崔波，李茹，史锦山. 基于智能合约的物联网访问控制系统 [J] 计算机工程, 2021, 47 (04): 21-31. (Zhang Jianghui, Cui Bo, Li Ru, Shi Jinshan. Access Control System of Internet of Things Based on Smart Contract [J]. Computer Engineering, 2021, 47 (04): 21-31.)

[25] Siris V A, Dimopoulos D, Fotiou N, *et al.* Decentralized authorization in constrained IoT environments exploiting interledger mechanisms [J]. Computer Communications, 2020, 152: 243-251.

[26] Kakei S, Shiraishi Y, Mohri M, *et al.* Cross-certification towards distributed authentication infrastructure: A case of hyperledger fabric [J]. IEEE Access, 2020, 8: 135742-135757.

[27] Honar Pajooh H, Rashid M, Alam F, *et al.* Multi-layer blockchain-based security architecture for internet of things [J]. Sensors, 2021, 21 (3): 772.

[28] Zhou Lijing, Wang Licheng, Ai Tianyi, *et al.* BeeKeeper 2. 0: confidential blockchain-enabled IoT system with fully homomorphic computation [J]. Sensors, 2018, 18 (11): 3785.

[29] Hou Lu, Zheng Kan, Liu Zhiming, *et al.* Design and prototype implementation of a blockchain-enabled LoRa system with edge computing [J]. IEEE Internet of Things Journal, 2020, 8 (4): 2419-2430.

[30] Yang Xinting, Zhang Song, Liu Jintao, *et al.* Deep learning for smart fish farming: applications, opportunities and challenges [J]. Reviews in Aquaculture, 2021, 13 (1): 66-90.

[31] Feng Yunhe, Niu Haoran, Wang Fanqi, *et al.* SocialCattle: IoT-based Mastitis Detection and Control through Social Cattle Behavior Sensing in Smart Farms [J]. IEEE Internet of Things Journal, 2021.

[32] Hang Lei, Ullah I, Kim D H. A secure fish farm platform based on blockchain for agriculture data integrity [J]. Computers and Electronics in Agriculture, 2020, 170: 105251.

[33] Lee S, Lee J, Hong S, *et al.* Lightweight end-to-end blockchain for IoT applications [J]. KSII Transactions on Internet and Information Systems (TIIS) , 2020, 14 (8): 3224-3242.

[34] 弋伟国，何建国，刘贵珊，康宁波. 区块链增强果蔬质量追溯可信度方法研究与系统实现 [J]. 农业机械学报, 2022, 53 (02): 309-315+345. (Yi Weiguo, He Jianguo, Liu Guishan, Kang Ningbo. Development and Implementation of Blockchain to Enhance Traceability and Reliability of Fruit and Vegetable Quality [J]. Transactions of the Chinese Society for Agricultural Machinery, 2022, 53 (02): 309-315+345.)

[35] Kara N, Cagiltay K. Smart toys for preschool children: A design and development research [J]. Electronic Commerce Research and Applications, 2020, 39: 100909.

[36] Yang Jian, Lu Zhihui, Wu Jie. Smart-toy-edge-computing-oriented data exchange based on blockchain [J]. Journal of Systems Architecture, 2018, 87: 36-48.

[37] Manzoor A, Samarin M, Mason D, *et al.* Scavenger Hunt: Utilization of Blockchain and IoT for a location-based Game [J]. IEEE Access, 2020, 8: 204863-204879.

[38] Pittaras I, Fotiou N, Siris V A, *et al.* Beacons and blockchains in the mobile gaming ecosystem: A feasibility analysis [J]. Sensors, 2021, 21 (3): 862.

[39] Farrokhi A, Farahbakhsh R, Rezazadeh J, *et al.* Application of Internet of Things and artificial intelligence for smart fitness: A survey [J]. Computer Networks, 2021: 107859.

[40] Jamil F, Iqbal N, Ahmad S, *et al.* Peer-to-peer energy trading mechanism based on blockchain and machine learning for sustainable electrical power supply in smart grid [J]. IEEE Access, 2021, 9: 39193-39217.

[41] Khan P W, Byun Y C, Park N. A data verification system for CCTV surveillance cameras using blockchain technology in smart cities [J]. Electronics, 2020, 9 (3): 484.

[42] Dileep G. A survey on smart grid technologies and applications [J]. Renewable Energy, 2020, 146: 2589-2625.

[43] Li Fangxin, Qiao Wei, Sun Hongbin, *et al.* Smart transmission grid: Vision and framework [J]. IEEE transactions on Smart Grid, 2010, 1 (2): 168-177.

[44] Zhao Wenting, Lv Jun, Yao Xilong, *et al.* Consortium Blockchain-Based microgrid market transaction research [J]. Energies, 2019, 12 (20): 3812.

[45] Li Y, Hu B. An iterative two-layer optimization charging and discharging trading scheme for electric vehicle using consortium blockchain [J]. IEEE Transactions on Smart Grid, 2019, 11 (3): 2627-2637.

[46] Li Yuancheng, Hu Baiji. A consortium blockchain-enabled secure and privacy-preserving optimized charging and discharging trading scheme for electric vehicles [J]. IEEE Transactions on Industrial Informatics, 2020, 17 (3): 1968-1977.

[47] Yu Yunjun, Guo Yanghui, Min Wwendong, *et al.* Trusted transactions in micro-grid based on blockchain [J]. Energies, 2019, 12 (10): 1952.

[48] Lohachab A, Garg S, Kang B H, *et al.* Performance evaluation of Hyperledger Fabric-enabled framework for pervasive peer-to-peer energy trading in smart Cyber–Physical Systems [J]. Future Generation Computer Systems, 2021, 118: 392-416.

[49] Jamil F, Kahng H K, Kim S, *et al.* Towards Secure Fitness Framework Based on IoT-Enabled Blockchain Network Integrated with Machine Learning Algorithms [J]. Sensors, 2021, 21 (5): 1640.

[50] Sciumè G, Palacios-Garcia E J, Gallo P, *et al.* Demand response service certification and customer baseline evaluation using blockchain technology [J]. Ieee Access, 2020, 8: 139313-139331.

[51] Wang Lognze, Jiao Shucen, Xie Yu, *et al.* A Permissioned Blockchain-Based Energy Management System for Renewable Energy Microgrids [J]. Sustainability, 2021, 13 (3): 1317.

[52] Nallaperuma D, Nawaratne R, Bandaragoda T, *et al.* Online incremental machine learning platform for big data-driven smart traffic management [J]. IEEE Transactions on Intelligent Transportation Systems, 2019, 20 (12): 4679-4690.

[53] Djahel S, Doolan R, Muntean G M, *et al.* A communications-oriented

perspective on traffic management systems for smart cities: Challenges and innovative approaches [J]. IEEE Communications Surveys & Tutorials, 2014, 17 (1): 125-151.

[54] Feng Qi, He Debiao, Zeadally S, *et al.* BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks [J]. IEEE Transactions on Industrial Informatics, 2019, 16 (6): 4146-4155.

[55] Li Wanxin, Guo Hao, Nejad M, *et al.* Privacy-preserving traffic management: A blockchain and zero-knowledge proof inspired approach [J]. IEEE Access, 2020, 8: 181733-181743.

[56] Luo Gege, Shi Mingxian, Zhao Caidan, *et al.* Hash-Chain-Based Cross-Regional Safety Authentication for Space-Air-Ground Integrated VANETs [J]. Applied Sciences, 2020, 10 (12): 4206.

[57] Buzachis A, Celesti A, Galletta A, *et al.* A multi-agent autonomous intersection management (MA-AIM) system for smart cities leveraging edge-of-things and Blockchain [J]. Information Sciences, 2020, 522: 148-163.

[58] Mbarek B, Jabeur N, Pitner T, *et al.* Empowering communications in vehicular networks with an intelligent blockchain-based solution [J]. Sustainability, 2020, 12 (19): 7917.

[59] Xiao Yonggang, Liu Yanbing, Li Tun. Edge computing and blockchain for quick fake news detection in IoV [J]. Sensors, 2020, 20 (16): 4360.

[60] Chen Wuhui, Chen Yufei, Chen Xu, *et al.* Toward secure data sharing for the IoV: a quality-driven incentive mechanism with on-chain and off-chain guarantees [J]. IEEE Internet of Things Journal, 2019, 7 (3): 1625-1640.

[61] Gao Feng, Zhu Liehuang, Shen Meng, *et al.* A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks [J]. IEEE network, 2018, 32 (6): 184-192.

[62] Chiu Weiyang, Meng Weizhi. EdgeTC-a PBFT blockchain-based ETC scheme for smart cities [J]. Peer-to-Peer Networking and Applications, 2021: 1-13.

[63] Bartolomeu P C, Vieira E, Ferreira J. Pay as You Go: A Generic Crypto Tolling Architecture [J]. IEEE Access, 2020, 8: 196212-196222.

[64] Lee Y, Jeong S, Masood A, *et al.* Trustful Resource Management for Service Allocation in Fog-Enabled Intelligent Transportation Systems [J]. IEEE Access, 2020, 8: 147313-147322.

[65] Lee D, Lee S H, Masoud N, *et al.* Integrated digital twin and blockchain framework to support accountable information sharing in construction projects [J]. Automation in construction, 2021, 127: 103688.

[66] Haaskjold H, Andersen B, Langlo J A. Dissecting the project anatomy: Understanding the cost of managing construction projects [J]. Production Planning & Control, 2021: 1-22.

[67] Suliyanti W N, Sari R F. Blockchain-Based Implementation of Building Information Modeling Information Using Hyperledger Composer [J]. Sustainability, 2021, 13 (1): 321.

[68] Elghaish F, Abrishami S, Hosseini M R. Integrated project delivery with blockchain: An automated financial system [J]. Automation in construction, 2020, 114: 103182.

[69] Yang R, Wakefield R, Lyu S, *et al.* Public and private blockchain in construction business process and information integration [J]. Automation in construction, 2020, 118: 103276.

[70] Sheng Da, Ding Lieyun, Zhong Botao, *et al.* Construction quality information management with blockchains [J]. Automation in construction, 2020, 120: 103373.

[71] Yuan Pu, Xiong Xiong, Lei Lei, *et al.* Design and implementation on hyperledger-based emission trading system [J]. IEEE Access, 2018, 7: 6109-6116.

[72] Hu Zhou, Du Yuhao, Rao Congjun, *et al.* Delegated Proof of Reputation Consensus Mechanism for Blockchain-Enabled Distributed Carbon Emission Trading System [J]. IEEE Access, 2020, 8: 214932-214944.

[73] Che Zheng, Wang Yu, Zhao Juanjuan, *et al.* A distributed energy trading authentication mechanism based on a consortium blockchain [J]. Energies, 2019, 12 (15): 2878.

[74] Silva F C, A Ahmed M, Martínez J M, *et al.* Design and implementation of a blockchain-based energy trading platform for electric vehicles in smart campus parking lots [J]. Energies, 2019, 12 (24): 4814.